UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/515,384	02/29/2000	Mary Ellen Zurko	C99021US	1649

22879 7590 01/04/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DARROW, JUSTIN T	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/515,384	ZURKO ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-27 and 29-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-27,29-32 and 35-40* is/are rejected.

7)☒ Claim(s) *33 and 34* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been presented for examination. Claims 1-20 have been canceled and new claims 21-28 have been added in a preliminary amendment filed 02/29/2000. Claim 28 has been canceled in an amendment filed 04/22/2004. Claims 21 and 24-27 have been amended and new claims 29-40 have been added in an amendment filed 09/17/2004. Claims 21-27 and 29-40 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/17/2004 has been entered.

Priority

3. Acknowledgment is made that the instant application is a division of Application No. 07/479,666, filed 02/13/1990, now U.S. Patent No. 6,507,909 B1.

Drawings

4. The drawings were received on 04/22/2004. These drawings are approved.

Response to Arguments

5. Applicant's arguments, see pages 9-14, filed 09/17/2004, with respect to the rejections of claims 21-27 under 35 U.S.C. § 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new grounds of rejection is made in view of Rosenthal, U.S. Patent No. 5,073,933 A.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 21, 23-26, 36, 38, and 40 are rejected under 35 U.S.C. 102(e) as being anticipated by Rosenthal, U.S. Patent No. 5,073,933 A.

As per claims 21, 24, 25, and 26, Rosenthal discloses a method, an automatic data processing machine programmed to execute a method, an automatic data processing machine comprising means for performing a method, and program storage devices readable by machine and tangibly embodying a representation of a program of instructions adaptable to be executed by the machine to perform a method for verifying the existence of a trusted path, comprising the following steps conducted in sequence:

(a) upon login by a user (see column 4, lines 17-19; when a user logs on; see column 3, lines 25-27; on a client on the local host (physically at the server) to change the access control list), assigning a process identifier to the user in the trusted computing environment (see column 4, lines 57-67; column 5, lines 1-3; adding an entry of a new authorized NetName identifying a process forming a session between a user and a server);

(b) storing the assigned process identifier in trusted memory (see column 4, lines 60-62; entries of new NetNames on a list; see column 2, lines 50-60; where the NetName is a physical quantity in the form of a magnetic signal stored; see column 3, lines 16-27; in a memory of the server computer secured by allowing only authorized hosts to connect to it);

(c) establishing a trusted path between the user and the trusted computing environment (see column 4, lines 64-67; setting up the session between the user running the server and the server);

(d) through the trusted path, displaying the process identifier to the user (see column 4, lines 60-62; returning the entries from the list on a ListHost request to the user for viewing); and

(e) upon the user's subsequent entry into the trusted computing environment, automatically displaying the process identifier to the user through the trusted path so that the user

is assured that the trusted path has been established (see column 5, lines 1-3; the user who has logged in is allowed to talk to the server which informs the host that the user has successfully logged on; see column 1, lines 55-56; displaying the NetName on the monitor to the user).

As per claims 23, 36, 38, and 40, Rosenthal additionally suggests:

that the process identifier is pronounceable (see columns 9 and 10, lines 14-16; Appendix A; user2netname as a pronounceable process identifier).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 22, 35, 37, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosenthal, U.S. Patent No. 5,073,933 A, as applied to claim 21 above, and further in view of Atalla, U.S. Patent No. 4,315,101 A.

Rosenthal describes the method of claim 21. He further discloses a composite process identifier (see column 4, lines 19-24; a credential as a composite process identifier containing the NetName of the client and a verifier including a timestamp to prevent replays). However, Rosenthal does not explicitly teach that the credential contains a randomly or pseudo-randomly generated group of alphanumeric characters. Atalla discloses that the process identifier is a

randomly generated group of alphanumeric characters (see column 3, lines 44-49; figure 1A, items 13 and 15; a user identifier code produced from a random number; see column 6, lines 64-68; column 7, lines 1-5; figure 5A, items 83 and 91). Additionally, Atalla points out that the random process identifier is produced each time (see column 4, lines 37-40; a new random number RD_y and new ID_y are produced to supplant the previous RN_x and ID_x). Thus, in both the methods of Rosenthal and Atalla, the process identifier is unique each time it is used. Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Rosenthal with the random process identifier of Atalla to prevent replay attacks (see Rosenthal, column 4, lines 19-24) and to improve security of data transmission operations without requiring transmission of matching encoding-decoding keys or of user-identification information (see Atalla, column 1, lines 56-63).

10. Claims 27 and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A.

As per claim 27, Rosenthal describes an apparatus comprising:

(a) an untrusted encrypting means for generating a trusted encrypted command (see column 4, lines 17-23; a host implementing a client process to encrypt a credential with a server's public key containing the NetName of the client as a process identifier; see column 4, lines 1-4; where the public key is given out by the server to persons whom he wishes to address messages to it so that they may encrypt the messages for his receipt only in a trusted manner);

(b) a trusted means for receiving the trusted encrypted command via a trusted path (see column 4, lines 24-26; the server receives the credential encrypted with the server public key in a trusted manner that it decrypts with its secret key);

(c) a means for displaying a representation of the trusted encrypted command to the user for verification (see column 5, lines 1-3; the user who has logged in is allowed to talk to the server which informs the host that the user has successfully logged on; see column 1, lines 55-56; displaying the NetName on the monitor to the user); and

(d) a means for executing the verified trusted parsed command (see column 5, lines 1-3; allowing the user who is logged in to talk to the server).

Although Rosenthal explains that the use of public key encryption is known in the art (see column 4, lines 10-16), he does not explicitly teach parsing.

Rivest et al. disclose public key encryption of a message by parsing (see column 4, lines 32-37; a conventional blocking means is utilized to break a message into block words before encoding, where the message is represented by a number outside the range 0 to (n – 1)).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the apparatus of Rosenthal with the parsing of Rivest et al. to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4).

As per claim 29, Rosenthal further specifies:

that the display means automatically displays the representation of the trusted parsed command to the user for verification (see column 5, lines 1-3; the user who has logged in is

allowed to talk to the server which informs the host that the user has successfully logged on without explicit action by the user; see column 1, lines 55-56; displaying the NetName on the monitor to the user).

As per claim 30, Rosenthal then points out:

a means for initially inputting a process identifier by the user (see column 3, lines 25-27; a user on a client on the local host (physically at the server) to change the access control list; see column 4, lines 57-67; column 5, lines 1-3; adding an entry of a new authorized NetName identifying a process forming a session between a user and a server); and

a memory for storing the process identifier (see column 4, lines 60-62; entries of new NetNames on a list; see column 2, lines 50-60; where the NetName is a physical quantity in the form of a magnetic signal stored; see column 3, lines 16-27; in a memory of the server computer secured by allowing only authorized hosts to connect to it),

where the representation of the trusted parse command displayed to the user for verification constitutes the process identifier (see column 4, lines 60-62; returning the entries from the list on a ListHost request to the user for viewing).

As per claim 31, Rosenthal discloses an apparatus for controlling the execution by a machine of a trusted command that is issued by a user (see column 3, lines 25-27; a user on a client on the local host (physically at the server) to change the access control list; see column 4, lines 57-67; column 5, lines 1-3; adding an entry of a new authorized NetName identifying a process forming a session between a user and a server) and

that is encrypted by an untrusted parsing means to generate an encrypted command (see column 4, lines 17-23; a host implementing a client process to encrypt a credential with a server's public key containing the NetName of the client as a process identifier; see column 4, lines 1-4; where the public key is given out by the server to persons whom he wishes to address messages to it so that they may encrypt the messages for his receipt only in a trusted manner), comprising:

(a) means, readable by the machine, for causing the machine to receive the encrypted command from the untrusted encrypting means (see column 4, lines 24-26; the server receives the credential encrypted with the server public key in a trusted manner that it decrypts with its secret key); and

(b) means, readable by the machine, for causing the machine to execute the trusted command (see column 5, lines 1-3; allowing the user who is logged in to talk to the server).

Although Rosenthal explains that the use of public key encryption is known in the art (see column 4, lines 10-16), he does not explicitly teach parsing.

Rivest et al. disclose public key encryption of a message by parsing (see column 4, lines 32-37; a conventional blocking means is utilized to break a message into block words before encoding, where the message is represented by a number outside the range 0 to (n – 1)).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the apparatus of Rosenthal with the parsing of Rivest et al. to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4).

As per claim 32, Rosenthal discloses an apparatus for controlling the execution by a machine of a trusted command that is issued by a user (see column 3, lines 25-27; a user on a client on the local host (physically at the server) to change the access control list; see column 4, lines 57-67; column 5, lines 1-3; adding an entry of a new authorized NetName identifying a process forming a session between a user and a server) and

that is encrypted by an untrusted parsing means to generate an encrypted command (see column 4, lines 17-23; a host implementing a client process to encrypt a credential with a server's public key containing the NetName of the client as a process identifier; see column 4, lines 1-4; where the public key is given out by the server to persons whom he wishes to address messages to it so that they may encrypt the messages for his receipt only in a trusted manner), comprising:

(a) means, readable by the machine, for causing the machine to receive the user identification data from the user (see column 4, lines 17-19; when a user logs onto the host, the user password which is entered by the user decrypts the user's secret key, identifying of the user);

(b) means, readable by the machine, for causing the machine to receive the encrypted command from the untrusted encrypting means (see column 4, lines 24-26; the server receives the credential encrypted with the server public key in a trusted manner that it decrypts with its secret key);

(c) means, readable by the machine, for causing the machine to perform a security check on the encrypted command (see column 4, lines 24-26; the server using its secret key to decrypt the credential; see column 4, lines 30-32; checking the credential against the network-wide database to determine the authorization of the particular user) and a security check on the user

identification data (see column 4, lines 26-30; the server using the client's public key to decrypt the verifier where decryption by the client's public key identifies the user); and

(d) means, readable by the machine, for causing the machine to execute the trusted command (see column 5, lines 1-3; allowing the user who is logged in to talk to the server).

Although Rosenthal explains that the use of public key encryption is known in the art (see column 4, lines 10-16), he does not explicitly teach parsing.

Rivest et al. disclose public key encryption of a message by parsing (see column 4, lines 32-37; a conventional blocking means is utilized to break a message into block words before encoding, where the message is represented by a number outside the range 0 to (n – 1)).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the apparatus of Rosenthal with the parsing of Rivest et al. to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4).

Allowable Subject Matter

11. Claims 33 and 34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter:

Claim 33 is drawn to an apparatus for controlling the execution by machine of a trusted command. The closest prior art, Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, disclose a similar apparatus. However, neither Rosenthal nor

Rivest et al. teach or suggest a means, readable by the machine, for causing the machine to receive a signal from the user signifying whether the displayed representation accurately represents the trusted command; and a means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command does not accurately represent the trusted command. These composite features explicitly recited in dependent claim 33 render it to have allowable subject matter.

Claim 34 is drawn to an apparatus for controlling the execution by machine of a trusted command. The closest prior art, Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, disclose a similar apparatus. However, neither Rosenthal nor Rivest et al. teach or suggest a means, readable by the machine, for causing the machine to receive a signal from a second user signifying whether the displayed representation accurately represents the trusted command; and a means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command does not accurately represent the trusted command. These composite features explicitly recited in dependent claim 34 render it to have allowable subject matter.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

December 26, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100